

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-027123

(43)Date of publication of application : 27.01.1998

(51)Int.Cl.

G06F 12/00  
G06F 3/06  
G06F 9/06  
G06F 12/14

(21)Application number : 08-182236

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 11.07.1996

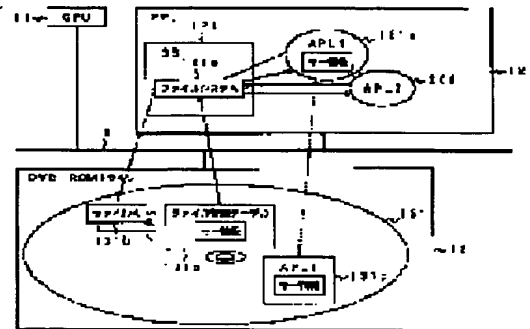
(72)Inventor : NAKAMURA SEIICHI

### (54) METHOD FOR PROTECTING COMPUTER SOFTWARE FROM COPYING

#### (57)Abstract:

PROBLEM TO BE SOLVED: To protect software from copying by restricting a program capable of reading out a file from a software distributing recording medium.

SOLUTION: When a reading request to a file 131b in a recording medium 131 is issued, an operating system 121 collates key information specified by a user program based on the reading request with key information set up as the attribute information of a corresponding file and judges the validity/ invalidity of file reading based on the collated result. Thereby a file reading request from a program 131a previously including the key information of the corresponding file registered in a file management table 131c and capable of issuing the key information at the time of receiving the file reading request is permitted but a file reading request from other programs can not be received.



#### LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-27123

(43) 公開日 平成10年(1998) 1月27日

(51) Int.Cl. <sup>8</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 12/00	5 3 7		G 0 6 F 12/00	5 3 7 A
3/06	3 0 4		3/06	3 0 4 M
9/06	5 5 0		9/06	5 5 0 G
12/14	3 2 0		12/14	3 2 0 F

審査請求 未請求 請求項の数12 O L (全 13 頁)

(21) 出願番号 特願平8-182236

(22) 出願日 平成8年(1996) 7月11日

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 中村 誠一

東京都青梅市末広町2丁目9番地 株式会  
社東芝青梅工場内

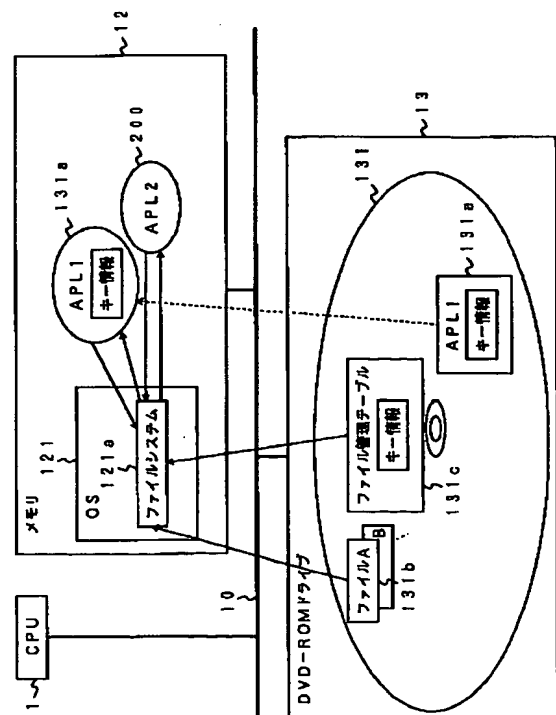
(74) 代理人 弁理士 鈴江 武彦 (外6名)

(54) 【発明の名称】 コンピュータソフトウェアのコピープロテクト方法

(57) 【要約】

【課題】 ソフトウェア配布用記録媒体からファイルを読み出すことができるプログラムを制限できるようにし、ソフトウェアのコピー防護を図る。

【解決手段】 オペレーティングシステム121は、記録媒体131のファイル131bに対する読み出し要求が発行されると、その読み出し要求でユーザプログラムによって指定されるキー情報とファイル管理テーブル131cに該当ファイルの属性情報として設定されているキー情報とを照合し、その照合結果に基づいてファイル読み出しの可否判定を行う。したがって、ファイル管理テーブル131cに登録されている該当ファイルのキー情報が予め組み込まれており、ファイル読み出し要求時にそのキー情報を発行することができるプログラム131aからのファイル読み出し要求については許可されるが、それ以外の他のプログラムからのファイル読み出し要求は受け付けられない。



## 【特許請求の範囲】

【請求項1】 コンピュータシステムで読み取り可能な情報記録媒体に記録されたソフトウェアの不正コピーを防止するコピープロテクト方法において、前記情報記録媒体に記録されているファイルに対するユーザプログラムからの読み出し要求に応答して、その読み出し要求でユーザプログラムから指定されたキー情報と、前記情報記録媒体内のファイルを管理するために前記情報記録媒体内に記録されているファイル管理テーブルに予め登録されているキー情報とを照合し、その照合結果に基づいてファイル読み出しを許可または禁止し、前記情報記録媒体のファイルを管理するファイル管理テーブルに登録されているキー情報を持つプログラムに対してのみ前記ファイルのファイル読み出しを許可できるようにしたことを特徴とするコピープロテクト方法。

【請求項2】 前記ファイル管理テーブルに登録されているキー情報を持つプログラムは、読み出し対象ファイルのファイル名と前記キー情報とを指定してファイル読み出しをオペレーティングシステムに要求するように構成されていることを特徴とする請求項1記載のコピープロテクト方法。

【請求項3】 前記キー情報の照合、およびその照合結果に基づく前記ファイル読み出しの許可または禁止の処理は、ユーザプログラムに対してファイルアクセスのためファイル管理サービスを提供するオペレーティングシステムによって実行されることを特徴とする請求項1記載のコピープロテクト方法。

【請求項4】 前記情報記録媒体に記録されたファイルはデータファイルであり、前記ファイル管理テーブルに登録されているキー情報を持つプログラムは、前記データファイルを使用して動作するアプリケーションプログラムであって、前記情報記録媒体に記録されていることを特徴とする請求項1記載のコピープロテクト方法。

【請求項5】 前記情報記録媒体に記録されたファイルは前記コンピュータシステムで実行可能なプログラムファイルであり、前記ファイル管理テーブルに登録されているキー情報を持つプログラムは、前記プログラムファイルをロードおよび実行するためのプログラムローダであって、前記情報記録媒体に記録されていることを特徴とする請求項1記載のコピープロテクト方法。

【請求項6】 前記ファイル管理テーブルに登録されているキー情報を持つプログラムには前記キー情報が暗号化されて組み込まれており、前記キー情報を持つプログラムは、その暗号化キー情報を前記情報記録媒体に記録されたソフトウェアを使用するために利用者から入力されたID番号を用いて復号化し、その復号化されたキー情報を用いてファイル読み出

しを要求することを特徴とする請求項1記載のコピープロテクト方法。

【請求項7】 コンピュータシステムで読み取り可能な情報記録媒体に記録されたソフトウェアの不正コピーを防止するコピープロテクト方法であって、

前記情報記録媒体には、  
コピー保護対象のデータファイルと、  
前記情報記録媒体に記録されているファイルそれぞれを管理するファイル管理テーブルであって、前記コピー保護対象のファイルについてはその属性情報としてキー情報が登録されているファイル管理テーブルと、  
前記コピー保護対象のデータファイルを読み出して使用するためのプログラムファイルであって、前記キー情報を指定してファイルオープン要求を発行するプログラムファイルとが記録されており、  
前記情報記録媒体に記録されているコピー保護対象データファイルに対するファイルオープン要求に応答して、そのファイルオープン要求で指定されたキー情報と、前記情報記録媒体内のファイル管理テーブルに登録されているキー情報とを照合し、  
その照合結果に基づいてファイルオープンを許可または禁止し、

前記キー情報が組み込まれた前記プログラム以外の他のプログラムからの前記コピー保護対象データファイルに対する読み出しを禁止できるようにしたことを特徴とするコピープロテクト方法。

【請求項8】 コンピュータシステムで読み取り可能な情報記録媒体に記録されたソフトウェアの不正コピーを防止するコピープロテクト方法であって、

前記情報記録媒体には、  
コピー保護対象のデータファイルおよびプログラムファイルと、  
前記情報記録媒体に記録されているデータファイルおよびプログラムファイルそれぞれを管理するファイル管理テーブルであって、前記コピー保護対象のファイルについてはその属性情報としてキー情報が登録されているファイル管理テーブルと、  
前記コピー保護対象のデータファイルおよびプログラムファイルを読み出して使用するためのプログラムローダであって、前記データファイルの読み出し時には対応するデータファイルのキー情報を指定してファイルオープン要求を発行し、前記プログラムファイルの読み出し時には対応するプログラムファイルのキー情報を指定してプログラムロードおよび実行の要求を発行するプログラムローダとが記録されており、  
前記情報記録媒体に記録されているコピー保護対象ファイルに対するファイルオープン要求に応答して、そのファイルオープン要求で指定されたキー情報と、前記情報記録媒体内のファイル管理テーブルに登録されているキー情報とを照合し、

その照合結果に基づいてファイルオープンを許可または禁止し、

前記情報記録媒体に記録されているコピー保護対象プログラムファイルに対するロードおよび実行の要求に応答して、そのロードおよび実行要求で指定されたキー情報と、前記情報記録媒体内のファイル管理テーブルに登録されているキー情報とを照合し、

その照合結果に基づいてプログラムファイルのロードおよび実行を許可または禁止し、

前記プログラムローダ以外の他のプログラムからの前記コピー保護対象データファイルおよびプログラムファイルの読み出し、および前記コピー保護対象プログラムファイルのロードおよび実行を禁止できるようにしたことを特徴とするコピープロテクト方法。

【請求項9】 コンピュータシステムで読み取り可能な情報記録媒体に記録されたソフトウェアの不正コピーを、オペレーティングシステムを用いて防止するコピープロテクト方法であって、

前記オペレーティングシステムには、ファイル名とキー情報とを指定可能なファイルオープンコマンドが用意されており、

前記情報記録媒体に記録されているファイルに対するユーザプログラムからのファイルオープン要求に応答して、そのファイルオープン要求で指定されたキー情報と、前記情報記録媒体内のファイルを管理するための情報を有し前記情報記録媒体内に記録されているファイル管理テーブルに予め登録されているキー情報とを照合し、

その照合結果に基づいて前記ユーザプログラムからのファイルオープンを許可または禁止し、

オペレーティングシステムによって実行される前記キー情報を使用したファイルオープンの許可または禁止処理によって、前記ファイル管理テーブルに登録されているキー情報を持つプログラムに対してのみ前記ファイルの読み出しを許可できるようにしたことを特徴とするコピープロテクト方法。

【請求項10】 コンピュータシステムで読み取り可能な情報記録媒体に記録されたソフトウェアの不正コピーを、オペレーティングシステムを用いて防止するコピープロテクト方法であって、

前記オペレーティングシステムには、ファイル名とキー情報とを指定可能なプログラムロードおよび実行コマンドが用意されており、

前記情報記録媒体に記録されているプログラムファイルに対するユーザプログラムからのプログラムロードおよび実行要求に응答して、そのロードおよび実行要求で指定されたキー情報と、前記情報記録媒体内のファイルを管理するために前記情報記録媒体内に記録されているファイル管理テーブルに予め登録されているキー情報とを照合し、

その照合結果に基づいて前記ユーザプログラムからのプログラムのロードおよび実行要求を許可または禁止し、オペレーティングシステムによって実行される前記キー情報を使用したプログラム実行の許可または禁止処理によって、前記ファイル管理テーブルに登録されているキー情報を持つプログラムに対してのみ前記プログラムファイルの実行を許可できるようにしたことを特徴とするコピープロテクト方法。

【請求項11】 ファイル名とキー情報とを指定可能なファイルオープンコマンドを有し、ユーザプログラムからのファイルオープン要求で指定されたキー情報と、オープン対象ファイルを管理するためのファイル管理テーブルに予め登録されているキー情報とを照合し、その照合結果に基づいてユーザプログラムからのファイルオープンを許可または禁止するオペレーティングシステムが搭載されたコンピュータで読み取り可能な記録媒体であって、

コピー保護対象のデータファイルと、前記情報記録媒体に記録されているファイルそれぞれを管理するファイル管理テーブルであって、前記コピー保護対象のファイルについてはその属性情報としてキー情報が登録されているファイル管理テーブルと、前記コピー保護対象のファイルを読み出して使用するためのプログラムファイルであって、前記コピー保護対象ファイルを読み出すとき、前記キー情報を指定してファイルオープンコマンドを発行するプログラムファイルとが記録されていることを特徴とする記録媒体。

【請求項12】 ファイル名とキー情報とを指定可能なファイルオープンコマンドを有し、ユーザプログラムからのファイルオープン要求で指定されたキー情報と、オープン対象ファイルを管理するためのファイル管理テーブルに予め登録されているキー情報とを照合し、その照合結果に基づいてユーザプログラムからのファイルオープンを許可または禁止するファイルオープン機能と、ファイル名とキー情報とを指定可能なプログラムロードおよび実行コマンドを有し、ユーザプログラムからのプログラムロードおよび実行要求で指定されたキー情報と、実行対象プログラムファイルを管理するためのファイル管理テーブルに予め登録されているキー情報とを照合し、その照合結果に基づいてユーザプログラムからのプログラム実行を許可または禁止するプログラム実行機能とを有するオペレーティングシステムが搭載されたコンピュータで読み取り可能な記録媒体であって、コピー保護対象のデータファイルおよびプログラムファイルと、

前記情報記録媒体に記録されているデータファイルおよびプログラムファイルそれぞれを管理するファイル管理テーブルであって、前記コピー保護対象のファイルについてはその属性情報としてキー情報が登録されているファイル管理テーブルと、

前記コピー保護対象のデータファイルおよびプログラムファイルを読み出して使用するためのプログラムローダであって、前記データファイルの読み出し時には対応するデータファイルのキー情報を指定してファイルオープン要求を発行し、前記プログラムファイルの読み出し時には対応するプログラムファイルのキー情報を指定してプログラムロードおよび実行の要求を発行するプログラムローダとが記録されていることを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明はコンピュータソフトウェアのコピープロテクト方法に関し、特にオペレーティングシステムのファイルシステムに用意した機能によってコンピュータソフトウェアのコピープロテクトを実現するコピープロテクト方法に関する。

【0002】

【従来の技術】一般に、パーソナルコンピュータやワークステーションなどにおいては、コンピュータソフトウェアの著作権および作成者の保護を図るため、様々なコピープロテクト技術が利用されている。コピープロテクトは、コンピュータソフトウェアの不正コピーを防止するための仕組みである。

【0003】かつては、コンピュータソフトウェアを記録したフロッピーディスクなどの記録媒体そのもののデータ格納形式を変更したり、その記憶媒体の記憶領域の一部に物理的な欠陥を施すなどの手法によってコピー防護が行われることもあった。しかし、これらの防護方法は、その媒体に格納されたコンピュータソフトウェアの正当な利用そのものに対して支障を来す場合があるなどの問題があり、最近ではほとんど利用されなくなってきたのが現状である。

【0004】このため、現在では、コンピュータソフトウェアの保護は、オペレーティングシステムのファイル管理機能によって提供されるファイルアクセス制御という形態でしか実現されていない。ファイルアクセス制御は、コンピュータシステムで管理されるファイルの属性をグループ共有ファイル、私的ファイルなどに分け、利用者IDとファイル属性との関係から、各ファイルに対してその読み出し、書き込み、実行などを制限するためのものである。各利用者は、自分が作成したファイルの読み出し、書き込みなどは自由に行うことができるが、他の利用者の私的ファイルに対するアクセスを行うことはできない。

【0005】以下、このファイルアクセス制御を使用したファイルアクセスの手順を説明する。通常、オペレーティングシステムでは、ファイルオープン、ファイルリード、ファイルクローズなどのサービスを提供している。ユーザプログラムは、このオペレーティングシステムのファイルサービス機能を利用して、ファイルをオー

ブンし、読み出すことができる。この場合、ファイル読み出し処理は、次のように行われる。

【0006】1. ユーザプログラムは、オペレーティングシステムに対し、特定のファイルのファイルオープンを要求する。

2. オペレーティングシステムは、ユーザプログラムからのファイルオープン要求に従い、ユーザプログラムの要求したファイルのファイル管理テーブルを取り出す。

【0007】3. オペレーティングシステムは、ユーザプログラムのユーザIDと、ファイル管理テーブル内のファイル属性情報に記された読み出し可能なユーザIDと比較することなどにより、指定されたファイルが、ユーザプログラムで利用可能かどうかを調べる。

【0008】4. 調べた結果、利用可能ならばユーザプログラムにファイル記述子を返すが、利用不可ならばその旨を伝え、ファイルオープンエラーとなる。

5. ユーザプログラムは、ファイルが利用可能ならば、オペレーティングシステムに対し、ファイル記述子と一緒にファイルリード要求を発行する。

【0009】6. オペレーティングシステムは、ユーザプログラムの要求に従い、記録媒体よりファイル内のデータを読み出す。

7. オペレーティングシステムは、読み出したデータをユーザプログラムに渡す。

【0010】このように、ファイルの読み出し要求に対する許可／不許可は、オペレーティングシステムがユーザ自身をユーザIDなどと呼ばれる識別子によって識別し、ファイル管理テーブル内の許可情報に記された読み出し可能なユーザIDと比較することにより行われる。

【0011】しかしながら、このようなユーザIDによるファイル保護は、複数の利用者によって1台のコンピュータを共有するといった環境下における私的ファイルの保護という点では有効であるが、不特定多数の利用者に配布するコンピュータソフトウェアの保護を図ることはできない。

【0012】なぜなら、不特定多数に配布するプログラムの場合には、ユーザIDで読み出し可能なユーザを指定することができないからである。例えば、CD-ROMなどに記録されているコンピュータソフトウェアは、どのユーザIDで利用されるか特定できないため作成時には、どのユーザIDでも読み出し可能にしか作成することができない。よって、すべてのユーザは、そのCD-ROMなどからプログラムファイルやデータファイルを読み出し、容易に複製を作成することができる。

【0013】特に、最近では、DVDなどの大容量記録メディアが開発されており、映画や、アニメーションなどをコンピュータで実行可能なコンピュータソフトウェアとしてDVDなどに記録して配布するという形態も考えられており、コンピュータソフトウェアの不正コピーを防御するための新たな対策が望まれている。

## 【0014】

【発明が解決しようとする課題】 上述したように、ユーザIDによるファイル保護は複数の利用者によって1台のコンピュータを共有するといった環境下における私的ファイルの保護という点では有効であるが、不特定多数の利用者に配布するコンピュータソフトウェアの不正コピーを防止することはできず、すべてのユーザは、CD-ROMなどのソフトウェア配布用の記録媒体からプログラムファイルやデータファイルを読み出し、容易にその複製を作成することができるという問題があった。

【0015】 この発明はこのような点に鑑みてなされたものであり、ソフトウェア配布用の記録媒体からプログラムファイルやデータファイルを読み出すことができるプログラムをその記録媒体に格納されたプログラムなどの特定のプログラムに制限できるようにし、正当なソフトウェアの利用に障害をもたらすことなく、利用者がCD-ROMなどで配布されたコンピュータソフトウェアを不正にコピーすることを防止することが可能なコピープロテクト方法を提供することを目的とする。

## 【0016】

【課題を解決するための手段】 この発明は、コンピュータシステムで読み取り可能な情報記録媒体に記録されたソフトウェアの不正コピーを防止するコピープロテクト方法において、前記情報記録媒体に記録されているファイルに対するユーザプログラムからの読み出し要求に回答して、その読み出し要求でユーザプログラムから指定されたキー情報と、前記情報記録媒体内のファイルを管理するために前記情報記録媒体内に記録されているファイル管理テーブルに予め登録されているキー情報とを照合し、その照合結果に基づいてファイル読み出しを許可または禁止し、前記情報記録媒体のファイルを管理するファイル管理テーブルに登録されているキー情報を持つプログラムに対してのみ前記ファイルのファイル読み出しを許可できるようにしたことを特徴とする。

【0017】 このコピープロテクト方法においては、ファイル読み出し要求時にユーザプログラムなどからキー情報を受け取り、そのキー情報と、ファイル管理テーブルに登録されている読み出し対象ファイルのキー情報との照合結果に基づいて、そのファイルのファイル読み出しが許可または禁止される。このため、保護対象のファイルが記録された記録媒体にそのファイルを使用するために格納されて配布されるプログラムなどのように、ファイル管理テーブルに登録されているキー情報が予め組み込まれて、ファイル読み出し時にそのキー情報を発行することができるプログラムからのファイル読み出し要求だけが許可され、システムに標準装備されたコピーツールなどのキー情報を知らない他のプログラムからのファイル読み出し要求は受け付けられない。

【0018】 よって、正当なソフトウェアの利用に障害をもたらすことなく、利用者がCD-ROMやDVDな

どで配布されたコンピュータソフトウェアを不正にコピーすることを防止することが可能となる。

【0019】 また、このようなキー情報の照合とそれによるファイル読み出しの許可／禁止の制御機能をオペレーティングシステムにそのファイルシステムの機能として用意しておくことにより、ソフトウェア配布用の記録媒体に記録するコンピュータソフトウェア側には、保護対象ファイルのキー情報が登録されたファイル管理テーブルと、そのキー情報を持つプログラムなどを用意するだけで済み、コピープロテクト可能なコンピュータソフトウェアを容易に開発することが可能となる。

【0020】 また、保護対象のファイルがデータファイルである場合には、そのデータファイルを使用して動作するアプリケーションプログラムに前記キー情報を組み込んでおけばよいが、プログラムファイル自体を保護する場合には、コピーされても支障がないような小さなプログラムローダを用意しておき、そのローダにキー情報を埋め込んでおくことが好ましい。この場合、プログラムローダについてはその複製を防止することはできないが、他のプログラムファイルについてはその複製から防護することができる。

【0021】 さらに、プログラムローダなどのプログラムに埋め込んでおくキー情報は何らかの形で暗号化しておき、そのプログラムは、その暗号化キー情報を記録媒体に記録されたソフトウェアを使用するために利用者から入力されたID番号を用いて復号化し、その復号化されたキー情報を用いてファイルオープンを要求するように構成することが好ましい。これにより、読み出し可能なプログラムファイルからキー情報が盗まれるといった事態を防ぐことが可能となる。また、ファイル管理テーブルのキー情報については、オペレーティングシステムの機能によってその読み出しを禁止することが可能である。

## 【0022】

【発明の実施の形態】 以下、図面を参照してこの発明の実施形態を説明する。図1には、この発明の一実施形態に係るコピープロテクト方法が適用されたコンピュータシステムの構成の一例が示されている。このコンピュータシステムは、例えばパーソナルコンピュータやワークステーションであり、図示のように、バス10、CPU11、メモリ12のほか、配布されたコンピュータソフトウェアを読み取るための機構として、DVD-ROMドライブ13が設けられている。CPU11は、このシステム全体の動作を制御するためのものであり、このシステムの主記憶として使用されるメモリ12上にロードされたオペレーティングシステム121や各種アプリケーションプログラム131a、200などを実行する。

【0023】 オペレーティングシステム121は、このコンピュータで実行される各種プログラムに対してプロセス管理、メモリ管理、ファイル管理などの機能を提供

するものであり、ファイル管理のためのファイルシステム121aには、この実施形態のコピープロテクト方法を実現するために、次の機能が実装されている。

【0024】1. ファイルシステムは、全てのユーザプログラムに対し、ファイル管理テーブル内のキー情報の読み出しを禁止する。

2. ファイルをオープンする場合、通常のファイルオープンコマンドの他に、ファイル名とキー情報を同時にオペレーティングシステムに知らせることができ新しいオープンコマンドをシステムコールとして有している。

【0025】このファイルオープンコマンドがユーザプログラムから発行されると、ファイルシステム121aは、ユーザプログラムから指定されたキー情報と、ファイル管理テーブルに登録されているオープン対象ファイルのキー情報とを照合し、その照合結果に基づいて、そのファイルのファイルオープンを許可または禁止する処理を行う。

【0026】また、オペレーティングシステム121には、プログラムファイルのロードおよび実行時にキー情報と共にプログラム名を指定できる機能もシステムコールとして用意されており、このロードおよび実行のコマンドがユーザプログラムから発行されると、オペレーティングシステム121は、ユーザプログラムから指定されたキー情報と、ファイル管理テーブルに登録されているオープン対象ファイルのキー情報とを照合し、その照合結果に基づいて、そのプログラムファイルのロードおよび実行を許可または禁止する処理を行う。

【0027】DVD-ROMドライブ13が読み込み可能なDVDなどの記録媒体131は、コンピュータソフトウェアの配布のために使用されるものであり、ここには、コンピュータソフトウェアとして、特定のキー情報が組み込まれたプログラムファイル131と、コピープロテクト対象の各種ファイル群131bと、記録媒体131上に記録された全てのファイルそれぞれの所在などを管理するためのファイル管理テーブル131cとが記録されている。

【0028】プログラムファイル131は、メモリ12にロードされてオペレーティングシステム121上で実行されるアプリケーションプログラムであり、ファイル群131bを利用して動作する。

【0029】プログラムファイル131は、ファイル群131bを読み出すときは、オペレーティングシステム121に対して、読み出し対象ファイルのファイル名とそのファイルに対応するキー情報とを指定してファイルオープンコマンドを発行するように構成されている。

【0030】ファイル管理テーブル131cは、ディレクトリとして使用されるものであり、図2に示されているように、記録媒体131上の各ファイルに対して、ファイル名、ファイルタイプ（ファイル拡張子）、ファイル属性、ポインタ情報、ファイル作成日時情報、ファイ

ルサイズ情報などを管理している。

【0031】ファイル属性には、ユーザIDを利用したファイルアクセス制御を行うための情報として隠しファイルやリードオンリーファイルの指定や、私的ファイル／グループ共有ファイルなどの区分と各区分に対してリード（r）、ライト（w）、実行（x）等の許可・禁止を指定する情報が必要に応じて設定されると共に、この実施形態のコピープロテクト方法を実現するために使用されるキー情報も設定される。

【0032】このキー情報は、コピープロテクト対象のファイルに対して予め登録されるものであり、前述したようにファイル群131bのコピープロテクトを図る場合には、図2に示されているように、ファイル群131bを構成するファイルA、B、に対して所定のキー情報（ここでは、K1、K2）が設定される。

【0033】また、ポインタ情報は、ファイルの実体が格納されている記録媒体131上の先頭位置を示すクラスタ番号などの情報である。次に、図3を参照して、キー情報を利用したコピープロテクトの原理を説明する。コピープロテクト対象のファイル群131bの読み出しは、以下の手順で行われる。

【0034】1. 記録媒体131からメモリ12上にロードされて実行されるプログラム131aが、ファイル群131b内の所定のファイルを読み出すときは、まず、ファイルシステム121aに対して、読み出し対象ファイルのファイル名とそのファイルに対応するキー情報とを指定してファイルオープンコマンドを発行する。

【0035】2. ファイルシステム121aは、このファイルオープン要求に回答して、要求されたファイルを管理しているファイル管理テーブル131cを取り出す。

3. 次いで、ファイルシステム121aは、指定されたファイルのキー情報と、プログラム131aから渡されたキー情報とを照合して、指定されたファイルがプログラム131aが読み出し可能なファイルであるか否かを調べる。

【0036】4. キー情報が情報が同じならば利用可能と判定され、ファイルシステム121aは、指定ファイルに対して割り当てたファイル記述子をプログラム131aに返す。一方、キー情報が違えば、ファイルシステム121aは、指利用不可の旨をプログラム131aに伝え、これによりファイルオープンエラーとなる。

【0037】5. プログラム131aは、ファイルが利用可能ならば、ファイルシステム121aに対し、ファイル記述子と一緒にファイルリード要求を発行する。

6. ファイルシステム121aは、プログラム131aの要求に従い、記録媒体131よりファイル内のデータを読み出す。

【0038】7. ファイルシステム121aは、読み出したデータをプログラム131aに渡す。このように、

キー情報の照合結果に基づいてファイルオープンの可否判定が行われるので、ファイル管理テーブル131cに登録されている該当ファイルのキー情報が予め組み込まれており、ファイルオープン要求時にそのキー情報を発行することができるプログラム131aからのファイルオープンについては許可されるが、例えば図1のプログラム200などのようにキー情報を知らないプログラムからのファイルオープン要求は受け付けられない。

【0039】よって、正当なソフトウェアの利用に障害をもたらすことなく、利用者がDVDなどの記録媒体131で配布されたコンピュータソフトウェアを不正にコピーすることを防止することが可能となる。

【0040】また、このようなキー情報の照合とそれによるファイルオープンの許可/禁止の制御機能をファイルシステム121aの中に用意しておくことにより、記録媒体131に記録するコンピュータソフトウェア側には、保護対象ファイルのキー情報が登録されたファイル管理テーブル131cと、そのキー情報を持つプログラム131aなどを用意するだけで済み、コピープロテクト可能なコンピュータソフトウェアを容易に開発することが可能となる。

【0041】また、コピープロテクト対象のプログラムファイルに対しては、前述のファイルオープンコマンドの許可/禁止の制御に加え、そのプログラムファイルに対するロードおよび実行コマンドの許可/禁止の制御についてもキー情報を用いて同様に行われる。

【0042】次に、図4のフローチャートを参照して、ファイルオープン要求時に実行されるファイルシステム121aの具体的な処理の手順について説明する。ファイルシステム121aは、ユーザプログラムからファイルオープンコマンドを受け取ると（ステップS11）、まず、そのファイルオープンコマンドで指定されたファイルを管理するファイル管理テーブルの該当ファイル属性情報を参照して、キー情報が設定されているか否かを判別する（ステップS12）。キー情報が設定されていない場合には、通常のファイルオープン処理が実行されて、ファイル記述子がユーザプログラムに返却される（ステップS13）。

したがって、コピープロテクト対象外のファイルである前述のプログラム131aについては無条件にその記録媒体131から読み出すことができる。

【0043】一方、ファイル管理テーブルの該当するファイル属性情報にキー情報が設定されている場合には、ファイルシステム121aは、ファイルオープンコマンドでキー情報が指定されたか否かを調べ（ステップS14）、指定されなかった場合にはその時点でファイルオープンエラーとなる。キー情報が指定されていた場合には、ファイルシステム121aは、指定されたキー情報とファイル管理テーブルの該当するキー情報とを照合する（ステップS16）。一致すれば通常のファイルオー

ブン処理が実行されて、ファイル記述子がユーザプログラムに返却される（ステップS13）が、不一致ならば、エラー処理が行われる。

【0044】次に、以上のようなコピープロテクト方法をソフトウェアベンダなどが利用して特定のファイルのコピープロテクトを図る場合に必要となる、コンピュータソフトウェアの格納形式について説明する。

【0045】図5においては、DVDなどの記録媒体131に格納された映像情報などを提供するためのデータファイル群のコピープロテクトを実現する場合に必要なソフトウェア構成が示されている。

【0046】記録媒体131には、プログラムファイル131aと、データファイル群113b-1、113b-2、113b-3と、ファイル管理テーブル131cが黒くされているが、ユーザが参照することが可能なファイルはプログラムファイル131aと、キー情報を除くファイル管理テーブル131cである。

【0047】記録媒体131にソフトウェアを記録して配布するソフトウェアベンダは、キー情報をプロテクト対象のデータファイル(A)113b-1、データファイル(B)113b-2、データファイル(C)113b-3毎に個別に作成、あるいはそれらデータファイルで共通のキー情報を作成して、ファイル管理テーブル131cの該当ファイルの属性情報として設定する。図5においては、データファイル(A)113b-1、データファイル(B)113b-2、データファイル(C)113b-3で共通のキー情報が用いられる場合が示されている。

【0048】そして、これらデータファイルを利用するプログラムファイル(A)131aの中には、データファイルをオープンするときにそのファイルに対応するキー情報が発行されるように、データファイル毎にそのキー情報が記述される。また、このプログラムファイル(A)131aについては、システム内の任意のプログラムによって読み出し可能なようにそのコピープロテクトのためのキー情報の設定は行わない。

【0049】このようなソフトウェア構成を採用することにより、データファイル群のコピープロテクトを容易に実現することができ、ソフトウェア作成者の意図しない不正コピーを防止することができる。

【0050】また、プログラムファイル(A)131aを例えば逆アセンブルする事などによってキー情報が盗まれるといった事態を防止するため、キー情報は何らかの形で暗号化してプログラムファイル(A)131aに埋め込んでおくことが好ましい。この場合、プログラムファイル(A)131aは、ファイルオープンコマンドを発行するときなどに、その暗号化キー情報を記録媒体131のソフトウェアを使用するために利用者から入力されたID番号を用いて復号化し、その復号化されたキー情報を用いてファイルオープンを要求する。これによ



り、読み出し可能なプログラムファイル131aからキー情報が盗まれるといった事態を防ぐことが可能となる。また、ファイル管理テーブル131cのキー情報については、オペレーティングシステムの機能によってその読み出しが禁止されているので、ファイル管理テーブル131cからキー情報が盗まれることはない。

【0051】図6のフローチャートには、プログラムファイル(A)131aによって実行されるキー情報復号化処理の手順が示されている。すなわち、プログラムファイル(A)131aは、まず、記録媒体131のソフトウェアを使用するためのID番号(例えば、記録媒体131に対して予め設定されているプログラムID番号、または利用者自身のユーザID番号など)がオペレーティングシステムがアプリケーションプログラム毎に管理する管理データ領域などに既に登録されているか否かを調べる(ステップS21)。登録済みの場合には、プログラムファイル(A)131aは、登録されているID番号と、オープン対象のファイルに対応する暗号化キー情報とに基づいて、その暗号化キー情報を復号化し(ステップS22)、そしてその復号化されたキー情報を用いてファイルオープンコマンドを発行する。

【0052】一方、未登録の場合には、プログラムファイル(A)131aは、前述したプログラムIDやユーザID等の入力を促すための画面表示などを行い、そして入力されたID番号を前述の管理データ領域に登録する(ステップS23、S24)。この後、プログラムファイル(A)131aは、登録されているID番号と、オープン対象のファイルに対応する暗号化キー情報とに基づいて、その暗号化キー情報を復号化し(ステップS25)、そしてその復号化されたキー情報を用いてファイルオープンコマンドを発行する。

【0053】次に、図7を参照して、記録媒体131に格納されたデータファイル群だけでなく、プログラムファイルについてのコピープロテクトも実現する場合に必要なソフトウェア構成を説明する。

【0054】記録媒体131にソフトウェアを記録して配布するソフトウェアベンダは、キー情報をプロテクト対象のプログラムファイル(A)131a-1、プログラムファイル(B)131a-2、プログラムファイル(C)131a-3、データファイル(A)113b-1、データファイル(B)113b-2、データファイル(C)113b-3毎に個別に作成、あるいはそれらファイルで共通のキー情報を作成して、ファイル管理テーブル131cの該当ファイルの属性情報として設定する。図7においては、ファイル毎に異なるキー情報が用いられている場合が示されている。

【0055】そして、これらプロテクト対象のファイルの他、それらプログラムやデータを読み出すために、コピーされても問題が少ない小さなプログラム(プログラムローダ)201を作成し、そのプログラムローダ20

1の中には、データファイルをオープンするときにそのファイルに対応するキー情報がオペレーティングシステムに対して発行されるようにデータファイル毎にそのキー情報が記述されると共に、プログラムファイルをメモリ上にロードして実行するときにそのファイルに対応するキー情報がオペレーティングシステムに対して発行されるようにプログラムファイル毎にそのキー情報も記述される。また、このプログラムローダ201については、システム内の任意のプログラムによって読み出しおよび実行可能なようにそのコピープロテクトのためのキー情報の設定は行わない。図7においては、ユーザが参照可能なファイルはプログラムローダ201と、キー情報を除くファイル管理テーブル131cだけであり、他のファイルを参照することはできない。

【0056】ユーザがプログラムローダ201を実行すると、プログラムローダ201内部に格納されたキー情報と共に、目的のプログラムを実行するオペレーティングシステムのサービスを呼び出し実行する。もし、ユーザが記録媒体131に格納されたデータやプログラムをコピーしようとした場合、ユーザは、キー情報を知ることができないのでファイルをオープンすることも、実行することもできないので、不正コピーを防止することができる。

【0057】また、プログラムローダ201を例えば逆アセンブルする事などによってキー情報が盗まれるといった事態を防止するため、キー情報は何らかの形で暗号化してプログラムローダ201に埋め込んでおくことが好ましい。この場合、プログラムローダ201は、ファイルオープンコマンドやプログラムロードおよび実行コマンドなどを発行するときなどに、その暗号化キー情報を記録媒体131のソフトウェアを使用するために利用者から入力されたID番号を用いて復号化し、その復号化されたキー情報を用いてそれらコマンドを発行する。これにより、読み出し可能なプログラムローダ201からキー情報が盗まれるといった事態を防ぐことが可能となる。また、ファイル管理テーブル131cのキー情報については、オペレーティングシステムの機能によってその読み出しが禁止されているので、ファイル管理テーブル131cからキー情報が盗まれることはない。

【0058】図8のフローチャートには、プログラムローダ201によって実行されるキー情報復号化処理の手順が示されている。すなわち、プログラムローダ201は、まず、記録媒体131のソフトウェアを使用するためのID番号(例えば、記録媒体131に対して予め設定されているプログラムID番号、または利用者自身のユーザID番号など)がオペレーティングシステムがアプリケーションプログラム毎に管理する管理データ領域などに既に登録されているか否かを調べる(ステップS31)。登録済みの場合には、プログラムローダ201は、登録されているID番号と、オープン/ロード対象

のファイルに対応する暗号化キー情報とに基づいて、その暗号化キー情報を復号化し（ステップS32）、そしてその復号化されたキー情報を用いてファイルオープンまたはロードおよび実行コマンドを発行する。

【0059】一方、未登録の場合には、プログラムローダ201は、前述したプログラムIDやユーザID等の入力を促すための画面表示などを行い、そして入力されたID番号を前述の管理データ領域に登録する（ステップS33、S34）。この後、プログラムローダ201は、登録されているID番号と、オープン/ロード対象のファイルに対応する暗号化キー情報とに基づいて、その暗号化キー情報を復号化し（ステップS35）、そしてその復号化されたキー情報を用いてファイルオープンまたはプログラムのロードおよび実行コマンドを発行する。

【0060】以上説明したように、この実施形態によれば、オペレーティングシステム121は、記録媒体131のファイル131bに対する読み出し要求が発行されると、その読み出し要求でユーザプログラムによって指定されるキー情報とファイル管理テーブル131cに該当ファイルの属性情報として設定されているキー情報とを照合し、その照合結果に基づいてファイル読み出しの可否判定を行う。

【0061】したがって、ファイル管理テーブル131cに登録されている該当ファイルのキー情報が予め組み込まれており、ファイル読み出し要求時にそのキー情報を発行することができるプログラム131aからのファイル読み出し要求については許可されるが、それ以外の他のプログラムからのファイル読み出し要求は受け付けられない。よって、正当なソフトウェアの利用に障害をもたらすことなく、利用者がDVDなどの記録媒体131で配布されたコンピュータソフトウェアを不正にコピーすることを防止することが可能となる。

【0062】また、プログラムファイルについては、そのロードおよび実行の要求についても正当なキー情報を持つプログラムからの要求しか受け付けられないので、不正なプログラムコピーを確実に防止することができる。

【0063】なお、この実施形態では、コンピュータソフトウェアを記録して配布する記録媒体としてDVDを

例示したが、CD-ROMやフロッピーディスクに記録されて配布されるソフトウェアについても全く同様のコピープロテクト方法を適用することができる。

【0064】

【発明の効果】以上説明したように、この発明によれば、オペレーティングシステムによるキーチェックに基づくファイル読み出しの可否制御により、ソフトウェア配布用の記録媒体からプログラムファイルやデータファイルを読み出すことができるプログラムをその記録媒体に格納されたプログラムなどの特定のプログラムに制限できるようになり、正当なソフトウェアの利用に障害をもたらすことなく、利用者がCD-ROMなどで配布されたコンピュータソフトウェアを不正にコピーすることを防止することが可能となる。

【図面の簡単な説明】

【図1】この発明の一実施形態に係るコピープロテクト方法を適用したコンピュータシステムの構成を示すブロック図。

【図2】同実施形態で使用されるファイル管理テーブルの構成を示す図。

【図3】同実施形態におけるキー情報を利用したコピープロテクト方法の原理を説明するための図。

【図4】同実施形態におけるファイルオープン要求時の処理手順を説明するためのフローチャート。

【図5】同実施形態のコピープロテクト方法でコピー防護される記録媒体内の第1のソフトウェア構成例を示す図。

【図6】図5のソフトウェア構成で使用される暗号化キーの復号化処理の手順を示すフローチャート。

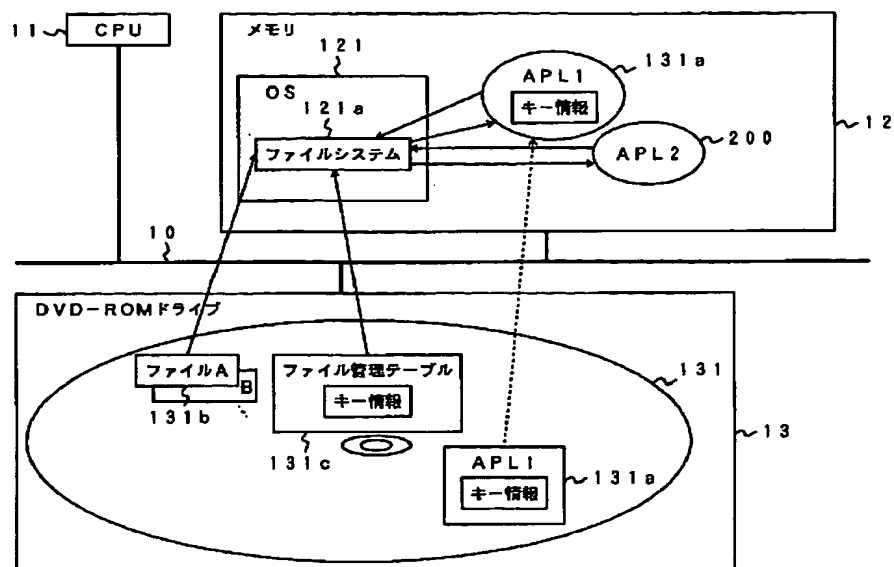
【図7】同実施形態のコピープロテクト方法でコピー防護される記録媒体内の第2のソフトウェア構成例を示す図。

【図8】図7のソフトウェア構成で使用される暗号化キーの復号化処理の手順を示すフローチャート。

【符号の説明】

11…CPU、12…メモリ、13…DVD-ROMドライブ、121…オペレーティングシステム、121a…ファイルシステム、131…記録媒体、131a…プログラム、131b…ファイル、131c…ファイル管理テーブル。

【図1】



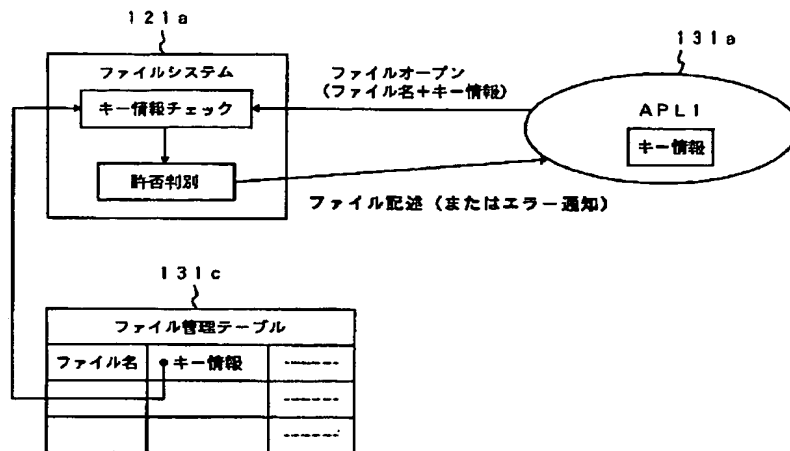
【図2】

ファイル管理テーブル

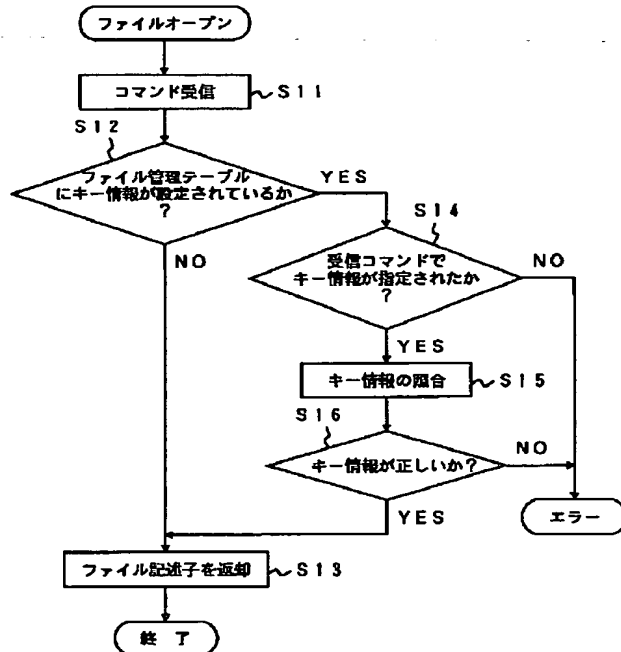
ファイル名	ファイルタイプ	ファイル属性		ポインタ	ファイル作成日時	ファイルサイズ
		r. w. x	キー情報			
ファイルA			K 1			
ファイルB			K 2			
APL 1			無			
⋮	⋮	⋮	⋮	⋮	⋮	⋮

131c

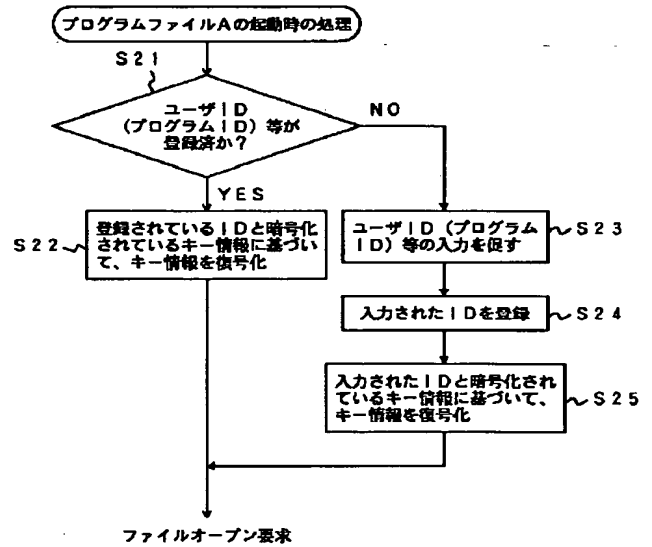
【図3】



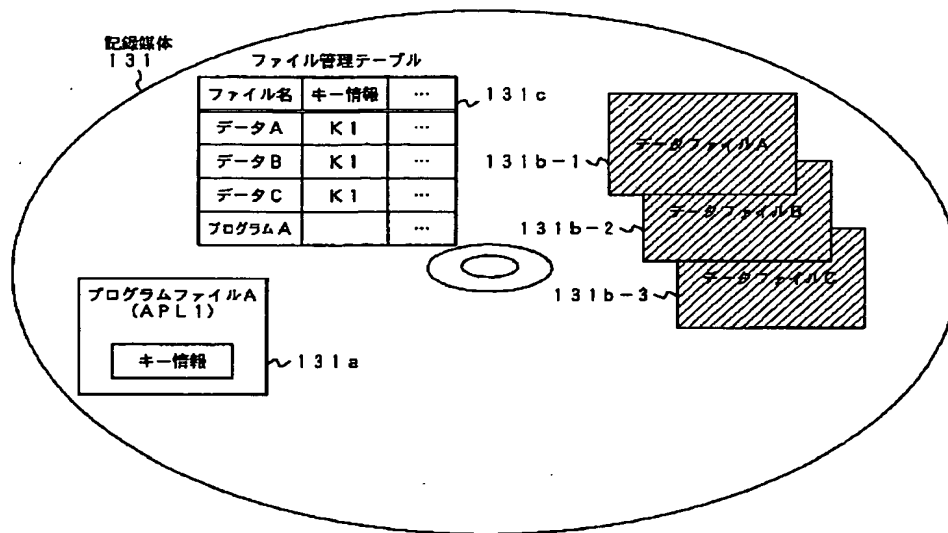
【図4】



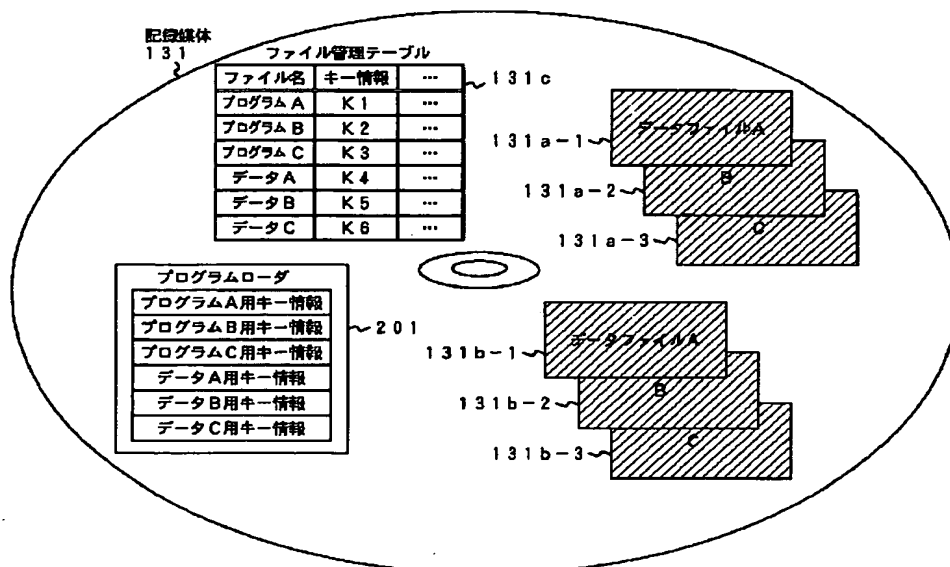
【図6】



【図5】



【図7】



【図8】

